AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

Claims 1 to 41 (Cancelled)

42. (New) A processor, comprising:

a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising:

a cipher core configured to cipher data received;

authentication cores connected to an authentication buffer and configured to authenticate the ciphered data received from the authentication buffer, at least two of the authentication cores each implementing a different authentication algorithm and requiring a different authentication algorithm block size; and

the authentication buffer connected to the cipher core and comprising buffer elements, each buffer element storing data corresponding to a respective one of the processing contexts and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer

configured to store the ciphered data received from the cipher core and to provide the ciphered data to the authentication cores each in an amount based on a corresponding authentication algorithm implemented.

43. (New) The processor of claim 42 wherein the processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the processing contexts with processing of the packet data in a second portion of the processing contexts.

44. (New) The processor of claim 42, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks.

45. (New) The processor of claim 42, wherein the crypto unit further comprises cipher cores configured to cipher data and the authentication buffer comprises authentication buffer elements.

46. (New) The processor of claim 45, further comprising a first multiplexer device connecting the cipher cores to the authentication buffer elements.

47. (New) The processor of claim 46, further comprising a second multiplexer device connecting the authentication buffer elements to the authentication cores.

48. (New) The processor of claim 45, wherein one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks.

49. (New) The processor of claim 45 wherein the number of the processing contexts does not equal a number of the cipher cores.

50. (New) The processor of claim 49 wherein the number of the processing contexts is six, a number of the buffer elements is six, the number of the cipher cores is four and the number of the authentication cores is five.

51. (New) The processor of claim 42 wherein the authentication buffer is configured to receive unciphered data and to provide the unciphered data to one of the authentication cores in an amount based on an authentication algorithm implemented.

52. (New) A processor disposed on an integrated circuit, comprising:

a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising:

cipher cores configured to cipher data received, one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks;

authentication cores connected to an authentication buffer and configured to authenticate the ciphered data received from the authentication buffer, at least two of the authentication cores each implementing a different authentication algorithm and requiring a different authentication algorithm block size; and

the authentication buffer connected to the cipher cores and comprising buffer elements, each buffer element storing data corresponding to a respective one of the processing contexts and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer configured to store the ciphered data received from the cipher cores and to provide the ciphered data to the authentication cores each in an amount based on a corresponding authentication algorithm implemented;

a first bus connecting the authentication buffer to the cipher cores; and

a second bus connecting the authentication buffer to the authentication cores.

53. (New) The processor of claim 52, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks.

54. (New) The processor of claim 52, further comprising:

a first multiplexer device connecting the cipher cores to the authentication buffer elements; and

a second multiplexer device connecting the authentication buffer elements to the authentication cores.

55. (New) The processor of claim 52 wherein the number of the processing contexts does not equal a number of the cipher cores.

56. (New) The processor of claim 52 wherein the number of processing contexts is six, a number of the buffer elements is six, the number of the cipher cores is four and the number of the authentication cores is five.

57. (New) The processor of claim 52 wherein the processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the processing contexts with processing of the packet data in a second portion of the processing contexts.

58. (New) A network switching device, comprising.

a processor disposed on an integrated circuit and comprising a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising:

a cipher core configured to cipher data received;

authentication cores connected to an authentication buffer and configured to authenticate the ciphered data received from the authentication buffer, at least two of the authentication cores each implementing a different authentication algorithm and one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks; and

the authentication buffer connected to the cipher core and comprising buffer elements, each buffer element storing data corresponding to a respective one of the processing contexts and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer configured to store the ciphered data received from the cipher core and to provide the ciphered data to the authentication cores each in an amount based on a corresponding authentication algorithm implemented.

59. (New) The device of claim 58 wherein the processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the processing contexts with processing of the packet data in a second portion of the processing contexts.

60. (New) The device of claim 58 wherein the crypto unit further comprises cipher cores configured to cipher data,

wherein one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks.

61. (New) The device of claim 60, further comprising:

a first multiplexer device connecting the cipher cores to the authentication buffer elements; and

a second multiplexer device connecting the authentication buffer elements to the authentication cores.

62. (New) The device of claim 58 wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server.

63. (New) A network, comprising.

a network switching device comprising a processor disposed on an integrated circuit comprising a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising:

a cipher core configured to cipher data received;

authentication cores connected to an authentication buffer and configured to authenticate the ciphered data received from the authentication buffer, at least two of the authentication cores each implementing a different authentication algorithm and requiring a different authentication algorithm block size; and

the authentication buffer connected to the cipher core and comprising buffer elements, each buffer element storing data corresponding to a respective one of the

processing contexts and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer configured to store the ciphered data received from the cipher core and to provide the ciphered data to the authentication cores each in an amount based on a corresponding authentication algorithm implemented.

64. (New) The network of claim 63 wherein the processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the processing contexts with processing of the packet data in a second portion of the processing contexts.

65. (New) The network of claim 63 wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks.

66. (New) The network of claim 63 wherein the crypto unit further comprises cipher cores configured to cipher data,

wherein one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks.

67. (New) The network of claim 63 wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server.

68. (New) An integrated circuit chip, comprising:

a processor comprising a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising:

cipher cores configured to cipher data received, one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks;

authentication cores connected to an authentication buffer and configured to authenticate the ciphered data received from the authentication buffer, at least two of the authentication cores each implementing a different authentication algorithm and one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks; and

the authentication buffer connected to the cipher cores and comprising buffer elements, each buffer element storing data corresponding to a respective one of the processing contexts and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer configured to store the ciphered data received from the cipher cores and to provide the ciphered data to the authentication cores each in an amount based on a corresponding authentication algorithm implemented.

69. (New) The integrated circuit chip of claim 68 wherein the number of the processing contexts does not equal a number of the cipher cores.

70. (New) The integrated circuit chip of claim 69 wherein the number of the processing contexts is six, a number of the buffer elements is six, the number of the cipher cores is four and the number of the authentication cores is five.

71. (New) The integrated circuit chip of claim 68 wherein the processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the processing contexts with processing of the packet data in a second portion of the processing contexts.

72. (New) A method of cryptographic data processing, comprising:

providing a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the respective data packet, the crypto unit comprising cipher cores, authentication cores; and an authentication buffer;

storing ciphered data in blocks having a predetermined size;

storing the data blocks in a first one of buffer elements in the authentication buffer based upon an associated one of the processing contexts, each buffer element storing data corresponding to a respective one of the processing contexts and having a size that is at least as

large as a largest authentication algorithm block size implemented by the authentication cores; and

providing the ciphered data to authentication cores each in an amount based on a corresponding authentication algorithm implemented by an associated authentication core, at least two of the authentication cores each implementing a different authentication algorithm and requiring a different authentication algorithm block size.

73. (New) The method of claim 72, further comprising ciphering data received in a first one of the cipher cores to form the ciphered data.

74. (New) The method of claim 72, further comprising ciphering data received using a first one of cipher algorithms to form the ciphered data.

75. (New) The method of claim 72, further comprising authenticating the ciphered data using the authentication algorithms.

76. (New) The method of claim 72, further comprising ciphering data using cipher cores, authenticating the ciphered data using authentication cores, and processing packets in parallel.

77. (New) The method of claim 72 wherein providing the ciphered data to authentication cores comprises providing the ciphered data to authentication cores comprising a first

authentication core to process data in 16-byte blocks and a second authentication core to process data in 64-byte blocks.

78. (New) The method of claim 72, further comprising providing the cipher cores comprising a first cipher core to processes data in 8-byte blocks and a second cipher core to process data in 16-byte blocks.